Energy
Regulatory Office

System Resilience – Challenges Related to the Digitalisation of the Energy Sector and Cyber Threats

Małgorzata Kozak
Director of Department of Market Development and Consumer Issues
Energy Regulatory Office of Poland

ERRA Energy Transition Committee Meeting
17 March 2026, Vilnius

System Resilience – Challenges Related to the Digitalisation of the Energy Sector and Cyber Threats

Digitalisation of the Energy Sector – Key Challenges

Report: *Assessment of the Digital Maturity of Electricity Market Companies in Poland (2023)*

Prepared by **ThinkTank** upon the request of the **Chancellery of the Prime Minister of Poland**

Key findings:

- energy companies possess **large volumes of data** that could support the development of new tools and processes; however, their use remains limited due to the lack of a **data-driven culture** and mature **data governance frameworks**
- the **overall level of advancement of IT systems and applications is relatively high**, but innovation activities are mainly focused on **operational improvements** rather than on projects creating **new value or business models**
- **data management and data governance structures** are still at an early stage of development. At the same time, companies will soon need to meet **additional requirements arising from new EU regulations**
- **digitalisation initiatives are not always implemented within a coherent strategy**, and activities carried out by individual organisational units often remain **siloed**

System Resilience – Challenges Related to the Digitalisation of the Energy Sector and Cyber Threats

Digitalisation of the Energy Sector – Key Challenges

- **integration of a growing share of renewable energy sources (RES) and distributed generation**
- **smart metering** - deployment, integration and effective use of data
- **cybersecurity of critical energy infrastructure**
- **modernisation of grid infrastructure**
- **management of large-scale data sets (Big Data)**
- **development of system flexibility and new electricity market models**
- **integration of electromobility with the power grid**
- **skills development and organisational culture change** - digitalisation is not only about technology
- **financing and the cost of the energy transition**
- **regulatory compliance and standardisation**

System Resilience – Challenges Related to the Digitalisation of the Energy Sector and Cyber Threats

Operation of Wind and Photovoltaic Farms

The operation of **wind and photovoltaic farms** is monitored and controlled through **industrial automation systems**.

Due to their **geographical dispersion**, the devices installed at these facilities enable **remote management of operational parameters**, diagnostics, service planning and incident response – often performed **from central dispatch centres or by external maintenance providers**.

Although individual installations usually have **relatively small generation capacities**, a **coordinated disruption of many such units** may have **serious consequences for the stability of the power system**.

Cybersecurity of renewable energy installations is important not only for the **companies that own and operate them**, but also for **distribution system operators (DSOs), the transmission system operator (TSO), and for citizens relying on a stable electricity supply**.

System Resilience – Challenges Related to the Digitalisation of the Energy Sector and Cyber Threats

Lessons from the cyberattack on the Polish energy system – 29 December 2025

Source: *Incident Report in the Energy Sector – 29 December 2025*
Prepared by CERT Polska / NASK and the Ministry of Digital Affairs of Poland
Energy Sector Incident Report - 29 December 2025 | CERT Polska

- **29 December 2025 – morning and afternoon hours:** coordinated cyberattacks were carried out in Polish cyberspace.
- **targets:**
  - ➢ wind farms and photovoltaic installations (at least **30 facilities**)
  - ➢ a **private company**
  - ➢ a **combined heat and power plant** serving more than **500,000 customers**.
- the incidents affected **both IT systems and industrial control devices**, which is a **very rare situation in previously documented cyberattacks**.

System Resilience – Challenges Related to the Digitalisation of the Energy Sector and Cyber Threats

Attack on wind and photovoltaic farms

- the attack had a **destructive character**
- **communication between the renewable energy installations and the distribution system operator (DSO)** was disrupted
- the attack affected **electric power substations**, known as **main grid connection points**, which communicate with the operator through the **SCADA system**
- the investigation showed that **many of these devices had been vulnerable in the past**, and the attackers had **administrator-level access to the devices at the moment of the attack**
- on the day of the attack, **all analysed devices were reset to factory settings**, which:
  - ➢ made it more difficult to restore the operation of the affected installations, and
  - ➢ was likely intended to **erase traces of the attack**

System Resilience – Challenges Related to the Digitalisation of the Energy Sector and Cyber Threats

Attack on a Large Combined Heat and Power Plant (CHP)

- **Objective:**
  the goal of the attack was to **irreversibly damage data stored on devices within the entity's internal network** by deploying **wiper-type malware** (software designed to destroy files or wipe disks in order to render devices inoperable or data unusable)

Preparation phase:

- the December attack was preceded by **reconnaissance activities conducted between March and July 2025**.
- during that period, the attackers gained **initial access to one of the devices**, which was later used as a **pivot point to connect to other machines within the network**.

Renewed malicious activity:

- towards the end of the year, **unauthorised activities were again observed within the organisation's infrastructure**, including:
  - ➢ reconnaissance,
  - ➢ credential theft,
  - ➢ unauthorised access to data,

System Resilience – Challenges Related to the Digitalisation of the Energy Sector and Cyber Threats

Attack on an Industrial Company

- the attackers attempted to **disrupt the operations of a manufacturing-sector company**.
- the actions were **coordinated with attacks on energy sector companies**.

However, the **target selection was opportunistic** – the company was chosen **not because of its strategic importance**, but because it was **relatively easy to compromise.**

The company **was not directly linked to the other attacked entities**

Initial Access Vector

- the attackers gained access through **Fortinet edge devices**
- the device had **known vulnerabilities in the past**, and its **configuration had previously been leaked and published**, including in posts on **online forums used by cybercriminal communities**
- after gaining access to the device, the attackers **introduced configuration changes designed to maintain persistent access**, even after user passwords

System Resilience – Challenges Related to the Digitalisation of the Energy Sector and Cyber Threats

Official Statement of the Government Plenipotentiary for Cybersecurity Regarding the Cybersecurity of Renewable Energy Sources (RES) – 19 January 2026

Key findings

- secure remote access: only VPN (site-to-site) or service access with MFA
- no direct internet exposure of OT devices or administrative interfaces
- strong authentication: remove default passwords and use unique accounts
- maintain asset inventory (devices, IP addresses, software versions)
- network segmentation and least-privilege access rules
- regular updates, configuration backups and security monitoring
- incident reporting to national CSIRT teams
- additional measures: log retention, IP allow-listing, private APN, CCTV and access control
- Komunikat Pełnomocnika Rządu do spraw Cyberbezpieczeństwa dotyczący cyberbezpieczeństwa OZE - Ministerstwo Cyfryzacji - Portal Gov.pl

www.ure.gov.pl

twitter.com/UREgovPL

linkedin.com/company/urząd-regulacji-energetyki/

Energy
Regulatory Office

Vilnius 2026